Noah Sunder Raj * et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.6, Issue No.3, April - May 2018, 8199-8200.

Secure Messaging –Cryptography And Middleware Queuing Using ISO 20022 Messaging Standards

NOAH SUNDER RAJ
M.Tech Student, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

G.MANOJ KUMAR
Assistant Professor, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

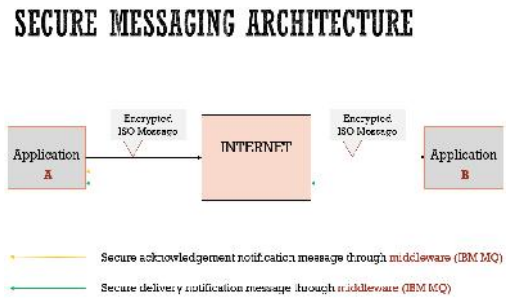
Abstract: **A secure messaging standard that acts as a platform for communication within and between applications is needed. Secure messaging uses criteria similar to SWIFT (Global Financial Interbank Financial Telecommunications), the international messaging system used for financial messaging worldwide. Secure Messaging can be used for secure communications within an application and between applications. It allows the structure of messages and message formats to be defined and delegated for use by the secure messaging community. Secure Messaging contains a series of features, a software that is enabled on the Internet, with a flexible structure that facilitates centralized or distributed publishing. Access is controlled by user access based on the smart card and messages are protected by standard encryption and authentication services according to ISO standards.**

Keywords: **Encrypted; Measurement; Sensor Networks; Decryption; Middleware;**

1. INTRODUCTION

Secure messaging can be used for secure communication within the organization and between two or more organizations. It allows the definition of message structures, message formats and authorization for the same use by the secure messaging community [1]. It has many features and is an Internet enabled program, with a flexible structure that facilitates centralized publication or distribution. Access is controlled by the user's access to the smart card and messages are protected by standard encryption and authentication services that comply with ISO standards. Both within and within the safe messages part are used by organizations to take full advantage of the secure messaging facilities they offer. The application also provides application software interfaces (APIs), which can be used to integrate current and future applications. Secure Messaging provides application software interfaces (APIs), which can be used to integrate current and future applications with Secure Messaging..

2. RESULTS



Here, Application A starts with a secure, encrypted message. This message is collected by the transmission process and placed in the remote queue for Application A. Here, the Application B queue places the remote message in the transmission queue between Application A and Application B [2]. The transmission queue submits the message through the Sender A channel. Additionally, Application A connects to Application B using the IP address and port number of the target application. The destination application receives the message through the receiver channel that is configured at the end. The receiving channel places this message in the local queue for Application B. The process of receiving Application B collects the message from the local queue and processes it. Once the message is processed by Application B, it is decrypted and displayed in the application's user interface. In this way, end messages between applications are successfully completed.

3. IMPLEMENTATION

Building Trusted Applications and Web: With modern electronic signatures in global and national commercial law, public-key encryption, digital signatures and digital certificates finally emerged as an integral part of the IT landscape. Although these technologies have existed for more than 20 years, this legislative measure will surely improve the activity of electronic commerce. Secure electronic business transactions, such as contracts, legal documents, insurance and bank loans, are now legally recognized [3][4]. To adapt to the realities of the market, other services may be needed, such as a non-repudiation service, a digital notary or a digital time-stamping service. These components, known as public key infrastructure (PKI), pave the way for secure communications within organizations and the public Internet.

Security and compliance: Maintain at all times the security of data. Banks need to demand stringent safety measures from suppliers and ensure new applications meet the latest and most rigorous

security standards [5]. Service Level Agreements (SLAs) are a must.

Reliability: Ensure that applications and data are always available in the event of a natural disaster or an unpredictable event. Applications need to have stringent SLAs in place, complete with guarantees, end-game scenarios and remedies if a provider fails to meet service levels.

Cloud management: Achieving vision and measuring performance is more difficult, especially if large banks are likely to obtain cloud services from multiple providers and use them for internal, external, external or public services. This may require a bank to manage multiple security systems, and the need to ensure that all parts of your business communicate with each other and, if necessary, with customers. The increased use of different technology infrastructures and a mix of different internal and external cloud environments means that secure messaging applications will need to develop fully developed cloud management platforms. There will be a need to ensure that banks can achieve cost savings and the benefits of flexibility in cloud computing.

Interoperability: Secure Messaging will need to ensure data and applications can be moved across cloud environments from a number of providers. They should look to develop a single interface and management layer that can work across different platforms internally and externally.

4. TECHNOLOGY IMPLEMENTED

The Application was developed mainly in Java and was used for communication within and between applications. The application server used in the project is the application server Tomcat version 7. The application uses an Oracle database to capture, store and analyze data [6]. The application uses the argument to move messages from one node to another. Java JRE is used to run the application. The application server is hosted on Windows 7, 8, 10 and the server's operating system, such as Windows Server 2008, 2012. Digital certificates are used to log on to the application that provides enhanced security at each node and increases reliability.

5. CONCLUTION

You are offering an open stack infrastructure solution as a service (IAAS) through a set of interconnected services. Each service provides an API that facilitates this integration. Open Shift is a platform as a Red Hat product. The program that runs an open-source name OpenShift service is available in Geetha. Developers can use Git to implement Web applications in different languages on the platform. Cloud computing is called Open Shift Enterprise. It should be noted that the integration of open stack with OpenShift will be a kind of integration of locomotives, because both have a rich array of features to offer. Then, as part of its future work, we would like to see how this Secure Messaging implementation platform can integrate and the additional features that can provide maintain current sound services.

6. REFERENCE

[1] Public Key Infrastructure: Building Trusted Applications and Web by John R. Vacca

[2] A.O. Freier, P. Karlton, and P.C. Kocher, “The SSL Protocol,” Internet-draft, draft-freier-ssl-version3-02.txt, November 1996.

[3] R. Thayer, N. Doraswamy, R. Glenn, (November 1998). IP Security Document Roadmap. IETF. RFC 2411, November 1998.

[4] S. Frankel, et al, Guide to IPsec VPNs, NIST Special Publication 800-77, December 2005.

[5] S. Nepal, J. Zic, S. Chen: A Contract Language for Service-Oriented Dynamic Collaborations. CollaborateCom 2008: 545-562 .

[6] J. Chan, G. Rogers, D. Agahari, D. Moreland and J. Zic, Enterprise collaboration contexts and their provisioning for secure managed Extranets, Proc. of IEEE WETICE 2006, p313-318.

